Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106

REPLY COMMENTS OF THE INTERNET COMMERCE COALITION

Jim Halpert
Sydney White
James Duchesne
500 8th Street, NW
Washington, D.C. 20004
(202) 799-4441

July 6, 2016

Executive Summary

The FCC NPRM proposes data privacy restrictions and mandates on ISPs that have never applied to the Internet and that exceed what is necessary to provide strong protections for consumers. Notably, the NPRM would combine an overly narrow de-identification definition that exempts only data that are aggregated and not "linkable" in theory to any person or device, with a sweeping opt-in consent requirement for non-de-identified ISP customer information, *regardless of sensitivity*, if used for any purpose other than service delivery or marketing "communications-related" services.

The FCC's departure from the FTC and Administration approach to privacy is not justified by unique privacy considerations. The NPRM and its supporters' comments overlook the fact that the proposed rules would harm competition and significantly restrict ISPs' First Amendment rights to communicate with their customers.

Instead of applying regulatory requirements based on the status of a company as an ISP, customer opt-ins should be required only for sensitive information, consistent with existing privacy regimes, consumer expectations, the technology-neutral FTC privacy framework, and the 2012 White House Privacy Report. By modeling the broadband privacy rules on the FTC's privacy framework and enforcing the rules itself, the Commission can still provide very strong protection of consumers' personal information, allow ISPs to use data in ways that consumers expect subject to a robust opt-out requirement, and avoid the First Amendment violations of a broad and strict opt-in regime.

As the FTC recommends in its comments, the Commission also should revise its data security and data breach proposals to focus robust protections and breach notice requirements on sensitive information. Protecting sensitive information will allow ISPs to best protect both consumers and the critical infrastructure that is their networks. Moreover, consistent with FTC

and state approaches to data security, the Commission should apply a “reasonableness” standard and not impose strict liability for data security.

TABLE OF CONTENTS

Page

I. Introduction

Nothing submitted in the record by defenders of the NPRM's proposed rules refutes the ICC's opening comments or justifies a different outcome than the "sensitive/non-sensitive data" approach that the ICC proposed. Bald assertions that all ISP data is sensitive (or should be considered sensitive because ISPs either cannot be trusted to identify information that is sensitive or should not be examining data) fail for reasons explained in Section II of these comments. Assertions that a bright-line opt-in rule applied to ISPs would be "simpler," not burdensome, or would avoid consumer confusion are equally misplaced.

We respectfully submit that the Commission can fulfill all the goals of Chairman Wheeler's high-level March 10th proposal[1] by following an approach that, consistent with the FTC privacy framework and the Administration's 2012 Privacy Report: (i) distinguishes clearly between sensitive and non-sensitive data; (ii) applies an opt-in consent requirement solely to the use and disclosure of sensitive data (and to retroactive material changes of the same practices); and (iii) provides consumers with clear and conspicuous notice so that they can easily exercise privacy choices with regard to non-sensitive data from which they can reasonably be identified. This would avoid significant unintended consequences and greatly reduce the risk that the Final Rule will be struck down for violating the First Amendment for reasons explained in Professor Laurence Tribe's comments.[2]

---

[1] *Chairman Wheeler's Proposal to Give Broadband Consumers Increased Choice, Transparency & Security with Respect to Their Data*, Fact Sheet (Mar. 10, 2016), http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0310/DOC-338159A1.pdf.

[2] Letter from CTIA, NCTA, and US Telecom, Docket No. 16-106 (May 27, 2016) (providing the analysis of Prof. Laurence H. Tribe) ("Tribe Comments").

Indeed, the FTC Bureau of Consumer Protection's comments strongly support the ICC's position that only sensitive information should be subject to an opt-in consent requirement (absent a retroactive material change) or trigger a breach notice requirement.[3] The FTC Comments show that the NPRM proposal, while sharing some high-level similarities to the FTC framework, is very different in key respects that make the proposed rules "not optimal."[4]

Companies routinely advertise to existing customers in both the online and offline worlds. The NPRM does not recognize that this advertising is mainstream, that with clear notice it is expected by customers in all sectors, and that it may provide real benefits to customers. The proposed rules would create serious obstacles to ISPs competing with other businesses to serve consumers in data-driven industries, particularly in online advertising. Countless companies touch the same consumer data and excessively burdensome FCC regulations should not be allowed to affect outcomes in this market.

Furthermore, the NPRM's departure from the existing successful FTC privacy framework and the framework endorsed by the White House[5] creates risk that it may be misinterpreted abroad in ways adverse to the interests of the United States. A number of commenters who support the proposed rule have advocated in Europe and, together with European privacy organizations, sent an open letter to the European Commission and Department of Commerce challenging the adequacy of the U.S. privacy framework.[6] They are very likely to cite any

---

[3] Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, at 19-20 (May 27, 2016) ("FTC Comments").

[4] *Id.* at 8.

[5] Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy P. 17 (Feb, 2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("White House Privacy Framework"). This report also contains the 2012 White House Privacy Bill of Rights.

[6] *See, e.g.* Letter to Secretary Pritzker and Commissioner Jourova, *available at* http://thepublicvoice.org/EU-US-NGO-letter-Safe-Harbor-11-15.pdf.

significant FCC departure from the established privacy framework as support for their arguments. As Professor Laurence Tribe's comments explain,[7] the NPRM raises serious First Amendment concerns. First, the proposed rule targets ISPs' ability to speak to a particular audience—their customers. The proposed rule is both speaker-based discrimination and a content-based restriction on ISPs' ability to speak, imposing different requirements for speech about *communications-related* services as opposed to a much broader category of *non-communications-related* services. In seeking to impose these restrictions on ISPs' ability to speak, the NPRM has not narrowly tailored the proposed rule to avoid unnecessarily limiting speech. Finally, a generalized assertion that the rule will protect privacy does not constitute a substantial government interest,[8] nor is a broad opt-in restriction on ISPs' ability to use and share data the sort of narrowly tailored solution that would survive First Amendment scrutiny in an Internet speech case. This record supports the argument that the proposed rule would be "more extensive than necessary" under the Supreme Court's *Central Hudson* test[9] and equally vulnerable under *Sorrell v. IMS*.[10]

II. The NPRM Applies An Overly Broad Opt-In Requirement

As the FTC comments make clear, the NPRM proposal departs sharply from the FTC's determination that protections should be tailored to the sensitivity of the information. The NPRM contradicts the FTC's long-held view that "all forms of personal information don't need

---

[7] Letter from CTIA, NCTA, and US Telecom, Docket No. 16-106 (May 27, 2016) (providing the analysis of Prof. Laurence H. Tribe) ("Tribe Comments").

[8] *U.S. West v. FCC*, 182 F.3d 1224, 1234-34 (10th Cir. 1999).

[9] *In re* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Notice of Proposed Rulemaking*, FCC 16-39, WC Docket No. 16-106, ¶ 302 (Mar. 31, 2016).

[10] *Sorrell v. IMS Health, Inc.*, 564 U.S. 552 (2011).

the same level of protection" and protections should be "appropriate to the risks."[11] The ICC agrees with the identification of specific examples of sensitive information included in the FTC Framework: financial data, health data, children's information, SSNs, and precise geolocation data. These categories of sensitive information should be subject to opt-in consent. With regard to data breach notification, a narrower subset of information should trigger notification, and data security requirements should be tailored to the sensitivity of the data. By contrast, non-sensitive data should be subject to implied or opt-out consent as explained in the FTC Comments.[12] These examples of sensitive information were reinforced by the FTC's comments and were echoed by the comments of many other parties.[13] Further, numerous federal and state laws hinge on the sensitivity of data to determine the appropriate level of protection.[14]

The NPRM proposal, if adopted, would reject the FTC's consistent determination, after considerable research and analysis that ISPs should *not* and need *not* be governed by a different set of standards with regard to how they handle broadband customer data. The FCC's imposition of different privacy rules on ISPs would create consumer confusion by displacing the simpler, unitary FTC framework that previously applied uniformly regardless of the type of company. Furthermore, the approach would run directly counter to consumer expectations. A May 2016 national survey by the Progressive Policy Institute (PPI) found that 83% of consumers expect that their information is protected based upon the sensitivity of the data, not the type of company

---

[11] Bureau of Consumer Protection Director Jessica Rich, *Keeping up with the Online Advertising Industry*, FTC (April 21, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry.

[12] FTC Comments at 22-23.

[13] *E.g.*, Comments of the Future of Privacy Forum, WC Docket No. 16-106, at 27 (May 27, 2016); Comments of Hughes Network Systems, LLC, WC Docket 16-106, at 4 n.11 (May 27, 2016); Comments of the National Cable & Telecommunications Association, WC Docket No. 16-106, at 44 (May 27, 2016) (NCTA Comments).

[14] *See, e.g.*, Cal. Civ. Code § 1798.82(h) (defining personal information for purposes of data breach notification).

that uses the data.[15] Instead , the NPRM's proposed rules would require a broad default opt-in requirement for *all* uses and sharing of *all* customer data, with limited exceptions, rather than narrowly tailoring its opt-in to the use and sharing of sensitive customer data. The proposed rules would impose opt-in requirements for a very broad range of data that do not apply under the FTC framework or the 2012 White House privacy framework. Furthermore, the proposed rules seem to exclude an exception for individual de-identified data, even though reasonably de-identified data does not raise privacy or security concerns.[16] In short, the NPRM over regulates in its definition of PII,[17] opt-in, and security and breach notice requirements.

In order to avoid unnecessarily limiting the use of data that does not pose a risk to consumers, the FTC recommends modifying the NPRM's proposed definition of PII as "any information that is linked or linkable to an individual"[18] by applying it only to information that is "*reasonably* linkable to an individual".[19] This would take into account whether a link to an individual "is practical or likely in light of current technology."[20] The Health Insurance Portability and Accountability Act (HIPAA) also includes a similar limitation in that there needs to be "a reasonable basis to believe the information can be used to identify the individual."[21] The final rule should fix this drafting oversight.

---

[15] *PPI Poll: Recent National Survey of Internet Users*, Progressive Policy Institute (May 26, 2016), http://www.progressivepolicy.org/issues/communications/ppi-poll-recent-national-survey-internet-users/.

[16] *See* Future of Privacy Forum Comments at 3-7.

[17] Maureen K. Ohlhausen, Commissioner, Federal Trade Commission, Reactions to the FCC's Proposed Privacy Regulations at the Advertising and Privacy Law Summit, at 6-7 (June 8, 2016) ("Ohlhausen Remarks").

[18] NPRM ¶¶ 57- 62.

[19] FTC Comments at 9.

[20] *Id.*

[21] 45 C.F.R. § 160.103.

The Public Knowledge comments joined by various other consumer and public interest groups argue that ISPs would have to manually inspect online content in order to implement a sensitivity-based approach.[22] This argument ignores the scope of the proposed rule, which applies to a much broader category of customer information than online content. More broadly, the comments overlook that there are established industry practices for prohibiting targeted advertising based on sensitive interest categories. Both ISPs and non-ISPs subject to the FTC Framework have been able to successfully operationalize and comply with sensitive/non-sensitive data distinctions for decades, and nothing has changed that would justify the major departure suggested by these commenters. A sensitivity-based approach would work in practice for ISPs, just as it works in practice for other entities subject to FTC Section 5 enforcement.

As discussed in the FTC's Report, only the use or disclosure of sensitive data—whether health data, financial data, children's data or precise location data—should trigger opt-in requirements, rather than applying an across the board opt-in.[23] And as the FTC's comments in this proceeding make clear, "Opt-out is sufficient for use and sharing of non-sensitive data."[24] This more measured approach would put the proposed rule on much more defensible ground, avoiding consumer confusion about the scope of an opt-in choice and avoiding First Amendment overbreadth in the NPRM proposal's sweeping marketing and advertising restrictions.

---

[22] Comments of Public Knowledge, the Benton Foundation, Consumer Action, Consumer Federation of America, and National Consumers League WC Docket No. 16-106, at 24-26 (May 27, 2016) ("Public Knowledge Comments"). Paul Ohm made a similar argument in his June 14, 2016 testimony before the House Energy & Commerce Communications Subcommittee that allowing ISPs to treat sensitive and non-sensitive information differently would allow ISPs to parse information in order to share some of it with third parties unlike other custodians of information who have a broad protection mandate.

[23] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers* at 47 (Mar. 2012) ("FTC Report").

[24] FTC Comments at 35.

In reply comments, Professor Paul Ohm attempts to discredit the FTC's sensitive data approach based upon three abstract arguments that do not fit the proposed rule.[25]

First, citing a single law review article discussing opt-ins for checking account overdraft fees,[26] Professor Ohm argues that ISPs will have significant flexibility in implementing an opt-in requirement so that the opt-in requirement would not be burdensome. Bear in mind that Professor Ohm's reply comments ask the Commission to apply an opt-in requirement for ISPs' use and disclosure of *all* data collected and for virtually *all* uses and sharing. In characterizing this purportedly minimal "burden," Professor Ohm thus ignores the First Amendment significance of this proposed across-the-board opt-in requirement. Moreover, the notice requirements in the proposed rule are highly prescriptive and do not give ISPs broad latitude to encourage consumers to opt-in as Professor Ohm argues in his reply comments. There is also reason to be very skeptical of an analogy to the single and very different context of a choice to opt in to pay overdraft fees.

There is a major difference between opting in to a program for a specific fee compared to requiring opt in for common uses of data that are typically included in a company's relationship with its customers. Further, the record evidence shows clearly that in most cases an opt-in regime results in very few consumers actually checking the box or executing the opt-in consent action,[27] which in this case would mean that consumers would no longer receive bundled discounts and other information regarding innovative new service offerings that they have come to expect and benefit from.

---

[25] Reply Comments of Paul Ohm, WC Docket No. 16-106 (June 22, 2016).

[26] *Id.* at 7-10.

[27] *E.g.*, Comments of AT&T Services, Inc., WC Docket No. 16-106, at 52-53 (May 27, 2016); Comments of Comcast Corp., WC Docket No. 16-106, at 26, 48-49 (May 27, 2016); NCTA Comments at 79-80.

Professor Ohm's second argument that a sensitivity-based approach would yield subjective interpretations that would vary by ISP relies entirely on the fact that self-regulatory regimes' have somewhat different interpretations of sensitive data.[28] As recognized in the 2012 FTC Privacy Staff Report, sensitivity does not always lend itself to a prescriptive bright-line rule. This is not an issue that is unique to ISPs, and Professor Ohm's observation does not provide a rationale for abandoning a contextual sensitivity-based approach to privacy. Most importantly, there is no reasonable basis for suggesting that FCC privacy rules that clearly define what sensitive data is subject to an opt-in consent requirement would be difficult to understand or difficult for ISPs to comply with on a consistent basis. Again, the FTC, which has extensively studied this issue for many years for both ISPs and non-ISPs, has consistently concluded that the best approach (*including for ISPs*) is to apply an opt-in consent requirement solely for sensitive data and that an opt-out consent requirement is sufficient for non-sensitive data when choice is necessary. The FTC repeated that very same conclusion and recommendation in its comments to the FCC in this proceeding.[29] Neither Professor Ohm nor any other commenter addresses, let alone refutes, the FTC's well-established conclusion and recommendation. The ICC respectfully submits that the FTC's views and recommendations on this critical issue should be given great weight.

Finally, Professor Ohm argues that an across-the-board opt-in requirement would be superior because it would be "simpler and more inexpensive to implement, and across the board rules lend themselves to consumer comprehensibility and confidence."[30] This argument, too, breezes over important facts. First, the CPNI rules have never been "simple" in the manner Ohm

[28] Ohm Comments at 11-12.

[29] FTC Comments at 15-16, 19-20.

[30] Ohm Comments at 11.

urges. They (as well as most other privacy laws) have always been a mixture of opt-in and opt-out requirements. This holds true for both the FTC or White House privacy frameworks. Second, obtaining the sort of specific opt-in consent contemplated by the proposed rule is expensive. It requires meticulous planning of what to request consent for, storing and cataloguing consents obtained, and associating those consents with specific data elements obtained in response to each consent given. There is nothing "simple" or "inexpensive" about this.

Finally, because the proposed rule would be very different in key respects from the FTC and White House privacy frameworks, and from virtually every other privacy law that applies to the Internet, consumer "comprehensibility" would actually be significantly *reduced* and consumer confusion would very likely *increase* by failure to adopt a clear sensitive/non-sensitive information distinction.

More broadly, no commenter effectively rebuts the common sense point endorsed by the FTC that the FCC should focus on "reasonable linkability" of data and not require data to be both aggregated and de-identified.[31] The FCC proposes an unnecessarily narrow approach to de-identification under the NPRM that fails to address de-identification of individualized information. By focusing only on de-identification of aggregated information, the FCC deviates from other US de-identification frameworks. This exclusive focus on aggregated data ignores that de-identified data, if de-identification is performed effectively in accordance with specific requirements, eliminates the need for customer consent because the privacy risks are no longer present.

---

[31] FTC Report at 21.

This narrow approach to de-identified data would restrict many uses of de-identified data that are beneficial to customers and ISPs, including those involving Big Data. Both the FTC, in its Big Data workshop and subsequent report[32] and the White House in its 2014 Big Data report[33] have recognized the beneficial uses of Big Data and the prospects for innovation using Big Data.

III. The NPRM Proposal Exceeds Permissible Restrictions on Commercial Speech Under the First Amendment

The *Central Hudson*, *Coors Brewing*, *US West*, and *Sorrell* line of cases shows how First Amendment criteria apply where an agency like the FCC is restricting commercial speech (e.g., advertising). In order to pass Constitutional review, the FCC must have a substantial interest in regulating the speech, regulate in a coherent manner that advances the substantial interest, and not suppress more speech than necessary to serve its governmental interest.[34] While the Commission understandably seeks to protect consumer privacy, the NPRM does not do so coherently or in a narrowly tailored manner.

The proposed rule applies to the use of data, sensitive or not, simply because it is handled by a particular speaker—an ISP. The proposal focuses on a particular type of speaker and not actual harms that the Commission seeks to address.[35] The court in the *US West* CPNI privacy decision stated that when a restriction of speech is imposed in order to protect privacy "the government must show the dissemination of the information desired to be kept private would

---

[32] FTC, *Big Data: A Tool for Inclusion or Exclusion*, at 12 (Jan. 2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

[33] Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, at 39-40 (May 2014), *available at* https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[34] *See U.S. West v. FCC*, 182 F.3d 1224 (10th. Cir. 1999).

[35] While data security and breaches are issues for *any* organization that collects personal information, severely restricting ISPs' ability to use data to advertise does not address the issue—especially because the Commission itself acknowledges that consumers want the information in these advertisements and find it useful. NPRM ¶ 12; s*ee also* Tribe Comments at 18-21.

inflict specific and significant harm on individuals . . . ."[36] The court went on to say that "[a] general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of a substantial state interest under *Central Hudson* for it is not based on an identified harm."[37] The NPRM has not identified any such specific harm and instead the FCC bases the proposed rules on consumers' alleged discomfort with ISPs using or sharing their non-sensitive information. Even these assertions are unsupported because the Pew study that the NPRM and its supporting commenters rely on addressed consumer concerns *in general* with using the Internet (which has a wide array of security risks), *not concern about ISP data practices*.[38]

Further, the NPRM proposal is not a narrowly tailored approach. The Commission does not explain why, for example, ISPs should be required to meet a higher opt-in consent standard for communications to customers regarding non-communications-related services as opposed to opt-out consent.[39] By distinguishing between *communications-related* and *non-communications-related* marketing and setting different standards for each, the Commission's proposal places restrictions on ISPs' communications with their customers based solely on the content of the communications. This type of restriction on speech must be narrowly tailored.[40] Indeed, as Professor Tribe points out, the Commission has actually acknowledged that the existing FTC

---

[36] *U.S. West* at 1235.

[37] *Id.*

[38] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Research Ctr. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

[39] NPRM ¶ 128; *see also* Tribe Comments at 30-32 (discussing the heavy burden to justify content-based restrictions). Again, there is no link to the harm the FCC is trying to address and the opt-in requirement. The "harm" in an ISP subscriber receiving a tailored advertisement is much different than, say, advertising based upon a consumer's surfing of sites related to a disease, which should require opt-in consent.

[40] *See Sorrell v. IMS Health, Inc.*, 564 U.S. 552, 571-72 (2011).

privacy framework is a workable, less restrictive solution to protecting consumer privacy that does not raise such serious First Amendment concerns.[41] In its comments, the ICC explained how the FTC framework protected consumers, appropriately focused additional protections on sensitive information, and did not unduly restrict ISPs' ability to communicate with their customers.[42] As it did in its comments, the ICC again calls on the Commission to model its final rule on the FTC's successful and constitutionally less burdensome privacy framework in its final rule.

IV. The Final Rule Should Rely on Established Notice and Choice Requirements

ISP customers had under the FTC framework and would certainly have under a final FCC rule consistent with that approach, control over their information with a clear notice and opt-out framework. Indeed, this is the framework that applies to other online companies and is the clear industry standard and norm that has developed consistent with the FTC framework. This opt-out industry norm is reflected in the Digital Advertising Alliance framework and the AdChoices program that provides advertising specific notice and control.[43]

Consistent with the FTC's well established framework, the Commission should focus on ensuring, in the context of ISP service, that consumers receive clear privacy notices and can readily exercise effective privacy choices. By contrast, the broad opt-in controls proposed in the NPRM would result in higher consumer costs as data-related revenue streams for ISPs are explicitly foreclosed.

The NPRM would likewise limit consumer choice. The NPRM opt-in proposal would have the readily foreseeable unintended consequences of restricting ISPs' ability to communicate

---

[41] Tribe Comments at 25 (citing NPRM ¶ 132).

[42] Comments of the Internet Commerce Coalition, WC Docket No. 16-106, at 2-7 (May 27, 2016).

[43] *See, e.g., Digital Advertising Alliance Consumer Choice Page*, DAA, http://www.aboutads.info/choices/.

with customers about special offers for non-communications-related services thereby resulting in fewer opportunities for customer discounts for cross service bundles and a more limited universe of services offered.

Other proposals by Public Knowledge and several other public interest commenters,[44] if reflected in the final rules, could likewise result in reduced consumer choice and less affordable broadband options. For example, foreclosing consumers from the option of obtaining discounted services in exchange for sharing any of their identifiable data for behavioral advertising would eliminate a significant component of consumer control and choice that can be an effective means for price conscious consumers to control costs. FTC Commissioner Maureen Ohlhausen has emphasized in many statements that high cost is the primary barrier to broadband uptake making ad supported services a valuable benefit to consumers.[45]

What is more, these proposals by Public Knowledge, *et. al.* ignore that under the Communications Act, the FCC is tasked principally with promoting competition and the expansion of broadband services, not regulating privacy without regard to those considerations.

V. Security and Breach Notice Requirements Must Be Commensurate with the Risk of Harm and Based on Reasonableness

The sensitive/non-sensitive data distinction is equally important with regard to the information security and data breach notice requirements in the proposed rule. The ICC agrees with the comments filed by the State Privacy and Security Coalition on the necessary distinction between sensitive and non-sensitive data with respect to data breach notification and data

---

[44] *E.g.*, Public Knowledge Comments at 6-9; Comments of Center for Digital Democracy, WC Docket No. 16-106, at 22 (May 23, 2016).

[45] Comments of FTC Commissioner Maureen K. Ohlhausen, WC-Docket 16-106, at 3 (May 27, 2016); Ohlhausen Remarks at 5.

security requirements.[46] There should be a likelihood of harm trigger that would warrant notification, where the sensitivity of the data would be an important factor in that analysis. Likewise, extensive record keeping requirements with regard to any access to or disclosure of customer data should not be required for data that is not sensitive.

As the FTC recommends, the Commission should also modify its proposal so that it does not impose strict liability for data security. Instead, the Commission should require "reasonable" data security and avoid establishing a static regulatory checklist for risk management and data security. Once again, this would align the Commission's approach with existing federal and state law.

Without these limitations, the final rule would conflict with state law principles, misalign security priorities for critical infrastructure providers, and needlessly raise the costs of providing broadband Internet access service.

VI. Conclusion

The ICC again urges the Commission to tailor the NPRM's proposals to align it with the FTC framework and the longstanding U.S. privacy regime. Focusing the proposed rule's opt-in requirements on truly sensitive data will best protect consumers, promote competition, and limit the possibility that the rule will impinge on ISPs' First Amendment rights to communicate with their customers. ICC also strongly recommends that the FCC amend the proposed rule's data security and data breach notification requirements to apply to sensitive data that triggers a likelihood of harm– and not simply all data—to best protect consumers and ISP critical infrastructure.

---

[46] Comments of State Privacy and Security Coalition, WC Docket No. 16-106, at 9-12 (May 27, 2016).

Respectfully submitted,

/s/

Jim Halpert
Sydney White
James Duchesne
Counsel to the Internet Commerce Coalition
DLA Piper LLP (US)
500 8th Street, NW
Washington, D.C. 20004
(202) 799-4441